EXHIBIT II.2 – INFORMATION SECURITY POLICIES AND PRACTICES

Custodianship of CalPERS information assets will only be permitted when sufficient protections are in place to protect the confidentiality, integrity, and availability of CalPERS information assets.

Entities using or storing CalPERS information assets as a result of contractual and/or other agreements will be considered custodians of that information asset(s).

Information assets include, but are not limited to records, files, paper documents, data, databases, systems, applications, and proprietary assets.

Solutions, as described in this document, include service and/or offerings from a contracted business partner.

To ensure appropriate protections of CalPERS information assets, the custodian must implement and comply with the requirements as detailed within this document. In addition, the vendor must provide documentation of compliance with CalPERS information security policies, practices, and standards. Documents provided by the vendor may include, but are not limited to, the request for proposal (RFP), the contract, and/or the statement of work.

The vendor must disclose all security, hosting, ownership and environment issues and processes that affect the migration, management, backup and recovery, security, or protection of CalPERS business data.

Identification

The solution must provide or support the use of a system entity identification mechanism that:

- Contains a registration process to define system entity profile information used in the identification, authentication, and authorization processes;
- Contains an identification process where data is transferred, presented, and/or collected to establish a claimed identity of a system entity; and,
- Contains a login process that enables a system entity to present an identity.

[For purposes of this document, system entity is an active element of a system (e.g., an automated process, a subsystem, a person or group of persons) that incorporates a specific set of capabilities.]

Authentication of System Entities

The solution must provide or support the acceptance of identity credentials from trusted and identified system entities to confirm/validate that identity before access is granted.

The solution must enforce an authentication strength that is commensurate with the related risk level and classification of the data, applications, and/or systems being accessed by the system entity to validate the claimed.

Security of Authentication Data

The solution must provide or support protection mechanisms that ensure identity and authentication data are kept private and secure, while in storage and/or transit, from unauthorized disclosure, access, modification, or destruction.

Non-Repudiation

The solution must provide or support the use of mechanisms that ensure against false denial of participation by a system entity while utilizing processes, data, resources, and systems.

Access Controls

The solution must provide or support mechanisms that prevent access to processes, data, resources, and systems by unauthorized system entities.

Confidentiality

All communications between users and systems using external shared networks (e.g., Internet) to access CalPERS information assets will be encrypted when passing through the external shared networks.

Vendor shall notify CalPERS of any unauthorized disclosure, modification, or destruction of confidential information by vendor, its officers, directors, employees, contractors, agents or third parties. Vendor shall make this notification promptly upon becoming aware of such disclosure, modification or destruction, but in any event, not later than four days after becoming aware of the unauthorized disclosure, modification, or destruction.

After such notification, vendor shall reasonably cooperate at vendor's expense with CalPERS to remedy or limit such disclosure or the effects of the disclosure. The provisions of this section will survive the expiration or termination, for any reason, of this Agreement.

The vendor must have a signed non-disclosure agreement (NDA) on file that binds the vendor to confidentiality.

Access to CalPERS information assets is limited to only those assets that are required by a requestor to conduct business.

Privilege Controls

The solution must provide or support privilege management mechanisms and capabilities (a high level authorization or set of authorizations to perform security-relevant functions) to confine a system entity to only those activities required to perform specified business and/or technical functions.

Relationship Management

The solution must provide or support the establishment and maintenance of controls that define privileges for system entities in accordance with their relationship to, and within, its organization.

Self Protection

The solution must provide or support the protection of processes, data, resources, and systems from exploitation, tampering, corruption, accidental, or malicious activities utilizing:

- Prevention mechanisms;
- Detection capability mechanisms; and
- Self recovery mechanisms in the event of failure such that all systems recover to a secured state.

Availability

The solution must provide or support mechanisms that ensure the availability of all processes, data, resources, and systems associated with the solution. Availability mechanisms include:

- Regularly scheduled and/or critical upgrades, software patches, and malware protections;
- Periodic backup of critical information assets; and
- Recovery of information assets back to a secured operational state.

Integrity

The solution must provide or support integrity mechanisms that ensure:

- Constant protection of processes, data, resources, and systems from unauthorized access or modification and to maintain consistency;
- Systems can perform their intended functions in an unimpaired manner;
- Authenticity and accuracy of all processes, data, resources, and systems;
- Backup and recovery of processes, data, resources, and systems; and,
- Constant protection of information assets while in transit or storage utilizing encryption mechanisms.

If CalPERS information assets switches from one location to another, the vendor is responsible for preserving the integrity of the information asset that is copied from the original site to the new one.

When a vendor uses a data storage provider (DSP) to host CalPERS information, the DSP must ensure accessibility, availability, integrity, consistency, security, compatibility, and compliance with CalPERS data formats and security practices.

Security Maintenance

The solution must implement mechanisms that maintain a consistent level of protections for processes, data, resources, and systems. Those protections include:

- Implementation of change management controls;
- Implementation of configuration management mechanisms;
- Implementation of mechanisms that maintain a consistent level of security during processes and activities associated with access to processes, data, resources, and systems;
- Implementation of storage and transmission security control protections during processes and activities associated with the transfer of information assets within, and external to, the organization; and
- Implementation of mechanisms that provide a consistent level of security in the event of system failure that assures recovery of processes, data, resources, and systems to the previously established safe state.

Account Management

The solution must implement the mechanisms to administer system entity accounts.

The solution must provide or support the ability to define and grant system entity access rights.

Audit and Accountability

The solution must implement audit and accountability control functions. Those functions include:

- Implementation of mechanisms that enable system usage review, security event logging, collection, storage, and monitoring;
- Implementation of information collection and reporting processes for detection, analysis, and response to security incidents and events;
- Implementation of mechanisms to protect security data from unauthorized access, modification and/or deletion; and,
- Implementation of the secure storage of audit logs, collect machine state and system usage information, and all items required for forensic investigations.

Infrastructure Security

The solution must provide a security plan that:

- Identifies the security services to ensure consistent and continued security of all devices, systems, network software, and operating systems used by, and interfacing with, the solution;
- Incorporates application software security services to ensure consistent and continued security of the organization's network and infrastructure;
- Details activities for emergency response, backup operations, and disaster recovery to ensure availability of critical system resources and facilitate the continuity of business operations; and,
- Describes the security services necessary to ensure consistent and continued security of the telecommunications components interfacing with the solution.